REMARKS

Claims 1-22 are pending in the application, of which Claims 1 and 12 are independent. Claims have been rejected under 35 U.S.C. 112, second paragraph, under 35 U.S.C. 102(e), and under 35 U.S.C. 103(a). Applicants respectfully traverse the rejections and request reconsideration.

Example Claim

Claim 1 is reproduced below for the convenience of the examiner. No amendments are being made.

1. An agent process for controlling access to digital assets in a network of data processing devices, the process comprising:

defining a point-of-use security perimeter that includes the operating system kernels of two or more data processing devices;

defining one or more policy violation predicates that serve to implement policy logic and that are asserted at the point-of-use of a digital asset upon an occurrence of a possible risk of use, outside of the security perimeter, of the digital asset by an end user;

sensing atomic events within an operating system kernel of a user client device, the atomic events being low level kernel events and being sensed upon actions relating to authorized access to a digital asset by the end user of the user client device;

aggregating multiple atomic level events to determine a combined event; and

asserting a policy violation predicate upon an occurrence of a combined event that violates a predefined digital asset usage policy that indicates a risk of use of the digital asset outside of the security perimeter.

Rejections Under 35 U.S.C. 112, Second Paragraph

Claims 1-22 have been rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Particularly, the Office states that the relationship between the claim elements *"defining a point-of-use security perimeter"* and *"use of the digital asset outside of the security perimeter"* would not be understood by one of ordinary skill in the art. Regarding these terms the Office asks how the digital asset could be used outside of the

perimeter if the security perimeter is based on the point-of-use. The following explains the quoted claim language.

Fig. 1 illustrates the concept of the point-of-use perimeter 200. Illustrated are example events that occur at the point-of-use of a digital asset and that may indicate a risk of using the digital asset outside of the security perimeter 200. Such events indicating a rink of use outside the perimeter 200 may include writing files to uncontrolled media, such as Compact Disk-Read Write (CD-RW) drives 204, Personal Digital Assistants (PDA) 206, Universal Serial Bus (USB) storage devices 208, wireless devices 212, digital video recorders 214, and printing 210 of files. These events may also include running external Peer-to-Peer (P2P) applications 201 and sending files via external e-mail applications 202. *See also* page 7, lines 1-8 of Applicants' specification.

Applicants respectfully point out that the claim language does not recite explicit use of a digital asset outside of the perimeter, but an indication of risk of such use. That is, the claims recite not a *"use of the digital asset outside of the security perimeter,"* but *"a risk of use of the digital asset outside of the security perimeter."* This risk is determined by sensing events at the point-of-use perimeter. For example, if an end-user attempts to write a file to a CD, a series of events will occur. Such events may include a series of small file reads, followed by writing to a temporary file for buffering of data, and then followed by a CD burn operation. These low-level events are sensed, a combined event is then determined from the low-level events, and if the combined event violates a policy that indicates a risk of use of the digital asset outside of the security perimeter (*e.g.*, the risk in this case being that the end-user would successfully burn the CD and walk away with the digital asset), then a policy violation predicate may be asserted, such as preventing completion of the CD burn operation. *See* page 13, lines 6-10 of Applicants' specification. Thus, use of the digital asset would not occur beyond the point-of-use perimeter, but activity that indicates a risk of such use occurs and is sensed at the perimeter.

Therefore, Applicants respectfully submit that the language of Claims 1 and 12 in view of the specification would be understood by one of ordinary skill in the art and is not indefinite. As such, Applicants respectfully request withdrawal of the rejections of Claims 1-22 under 35 U.S.C. 112, second paragraph. Applicants would, of course, gladly consider any amendments that the Office may suggest regarding the point-of-use perimeter.

Applicants appreciate the Office's indication that traversal of the rejections under 35 U.S.C. 112, second paragraph, would likely result in withdrawal of the rejections under 35 U.S.C. 102(e) and 35 U.S.C. 103(a). For the purpose of fully responding the Office Action, however, and because Applicants' previous arguments have not yet been addressed, Applicants present the following arguments, which are substantially similar to the arguments presented in their previous response.

Rejections Under 35 U.S.C. 102(e)

Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22 have been rejected under 35 U.S.C. 102(e) as being anticipated by Carter *et al.* (U.S. Pub. No. 2003/0051026, hereinafter "Carter").

In a previous response, Applicants submitted that Carter does not teach or suggest that atomic events are sensed *"within an operating system kernel of a user client device,"* as claimed in Claims 1 and 12, and provided two reasons: (1) Carter's NSSS does not sense events at an end user client device, and (2) the NSSS does not sense events within a kernel of an operating system of that device.

The Office then asserted that the events of Carter are sensed at a switch controlled by Carter's NSSS (*see* Carter, reference numeral 18 of Fig. 1). The Office also asserted that a workstation of Carter's Fig. 1 discloses the claimed end user client device. Applicants previously submitted that if Carter's NSSS senses events at the switch of Fig. 1, then the NSSS does not sense events at a workstation of Fig. 1. The Office responded to this by asserting that the claim language of *"from within an operating system kernel"* was open to alternate interpretations and that the Office did not take the interpretation previously argued by Applicants. The possible multiple interpretations have been addressed by Applicants' previous removal of the word "from" from the claims; thus, it is respectfully submitted that there should no longer be such alternative interpretations.

Further, the Office previously cited paragraph [0147] of Carter as disclosing that the sensing step of the NSSS is located within an operating system kernel, and the Office then cited paragraph [0810], which states that "[w]henever a user attempts a guarded operation ... the kernel relays the attempted operation to the watchdog system." The cited watchdog system is used to control access to files (*see* Carter, paragraph [0797] and [0810]). Access to the files is

based on a list of permissions and viewing rights (*see* Carter, paragraph [0809]), not based on an aggregation or combination of low-level events, as recited by Claims 1 and 12. Even if Carter's watchdog system were interpreted as disclosing the sensing of atomic events within an operating system kernel, the system bases its determination to grant a user access to a file based on a single event in which the user attempts to access the file. The watchdog system does not disclose *"aggregating multiple atomic level events to determine a combined event,"* as recited by Claim 1 and as similarly recited by Claim 12. Additionally, the watchdog system does not disclose *"asserting a policy violation predicate upon an occurrence of a combined event,"* as recited by Claim 1, or *"determin[ing] whether an aggregate event has occurred that violates a predefined digital asset usage policy,"* as recited by Claim 12. Further, the watchdog system does not disclose that any asserting or determining of a policy violation predicate is *"implemented in the operating system kernel,"* as recited by dependent Claim 2 and as similarly recited by dependent Claim 13.

Moreover, as previously submitted, Carter suggests that the NSSS is not part of an operating system kernel, because Carter discloses that the NSSS has a priority that is higher than that of a kernel (*see* Carter, paragraphs [0588] and [0589]) and that the NSSS may be in communication with and pass messages to the kernel (*see* Carter, paragraphs [0931] and [0936]), thus, suggesting that the NSSS and the kernel are separated. This is further supported by the fact that the watchdog system is not part of a kernel, but is only in communication with the kernel (*see* Carter, paragraphs [0810] and [0868]).

In addition, the claims recite in that the security perimeter is a *"point-of-use security perimeter that includes the operating system kernels of two or more data processing devices,"* as recited by Claim 1 and as similarly recited by Claim 12. Cited reference Carter discloses a traditional security system, which attempts to prevent access by outside users at a point of network access. Rather than establishing a perimeter at external points of access to a network, the claimed invention establishes a security perimeter at the points of digital asset use (*i.e.*, within the kernels of the user devices). Carter does not disclose this type of perimeter.

Therefore, Applicants respectfully submit that Claims 1, 2, 12, and 13 are novel and nonobvious over the cited art. Dependent Claims 3-5, 7, 8, 10, 11, 15, 16, 18, 19, 21, and 22 depend from independent Claims 1 or 12 and include the elements of Claims 1 or 12 presented

above as being novel and nonobvious over the cited art. Therefore, Applicants respectfully submit that these dependent claims are novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claims 1 and 12.

As such, Applicants respectfully request withdrawal of the rejections of Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22 under 35 U.S.C. 102(e).

Rejections Under 35 U.S.C. 103(a)

Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22 have been alternatively rejected under 35 U.S.C. 103(a) as being unpatentable by Carter in view of Danieli (U.S. Patent No. 6,510,513). Claims 6, 17, and 20 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Carter in view of Admitted Prior Art. Claim 9 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Carter in view of Danieli.

Even if Danieli were to be combined with Carter for the purpose of teaching the use of a digital asset outside of a security perimeter, as explained by the Office, the combination would not cure the deficiencies of Carter presented above with respect to independent Claims 1 and 12. Therefore, Applicants respectfully submit that Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22 are novel and nonobvious over such a combination of Carter and Danieli. As such, Applicants respectfully request withdrawal of the rejections of Claims 1-5, 7, 8, 10-13, 15, 16, 18, 19, 21, and 22 under 35 U.S.C. 103(a).

Dependent Claims 6, 9, 17, and 20 depend from independent Claims 1 or 12 and include the elements of Claims 1 or 12 presented above as being novel and nonobvious over the cited art. Therefore, Applicants respectfully submit that those dependent claims are novel and nonobvious over the cited art for at least the same reasons as presented above for independent Claims 1 and 12. As such, Applicants respectfully request withdrawal of the rejections of Claims 6, 9, 17, and 20 under 35 U.S.C. 103(a).

CONCLUSION

In view of the above remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By _____

Patrick A. Quinlan
Registration No. 61,287
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133

Date: 10/5/09